Sirtfi WG google folder:

https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDaIbqju40hOhUR

Current Task List

Who	What	When	Status
Nicole	FOs don't sign up for Sirtfi - create a template / criteria for involving them in incident response (i.e. get FOs to declare what they are doing and start actively monitoring this). Also encompasses defining what FOs should be doing during incidents.	In Progress	Raised at Steering Committee, small WG created.
Nicole	Peruse NGI Trust funded projects to identify any that may be relevant for Sirtfi.		
Christos	Propose a REFEDS 2020 Work plan item focused on understanding and potentially "regulating" proxy IdPs.		Closed
David G, Uros, **Sven**	Improve sharing procedures in AARC DNA3.2 paper by folding in experience from EGI.	Expected Dec 19, 2019	Delivered in FIR - Extending Sharing Procedures
Mario	Ask Dick Visser about taking control of sirtfi.org and CC Nicole		
Tom	Agendize review of educational materials to see if we're done with that Phase 2 deliverable.		
Tom	See about TrustedCI assistance with an IR wiki	Jan 30, 2020	Shared feedback with WG on Jan 28, 2020
Uros, Tom	Provide initial considerations of establishing channels for incident response, and how can the communication be coordinated (considering edugain csirt)	Feb 13, 2020	To be discussed in the context of the eduGAIN support security team's IR communications workflow

February 27, 2020

Attending: Sven, Romain, Tom, Maarten Kremers, Alan, Uros, Marina, Hannah, Shannon, Dave K, Christos

Regrets: David G, Laura P, Daniel Kouril

Agenda:

1. Any takeaways for the WG from the FIM4R and TIIME meetings last week?
2. Continue WG review and feedback on eduGAIN Security Incident Response Communication Workflow.
3. Compare/contrast ir_flowchart-1.pdf with checklist at the bottom of eduGAIN Security Incident Response Communication Workflow. Pick one over the other, merge somehow, or other alternative?
4. Does the WG believe that the above sufficiently fulfill its deliverable of "Define incident response procedures for federations, including communication templates, and support the community in their adoption"?
    a. If so, how should we help prepare everyone to play their IR roles?
5. Next steps for improving the AARC DNA3.2 paper.
6. AOB

No notables for this WG from FIM4R/TIIME last week.

Lots of good discussion centered around some of Marina's comments in the doc. Among the items we focused on are:

- Making clear that these procedures augment and don't supercede established local procedures.
- Identifying the current role of Sirtfi standing in these procedures.
- Absence of MUSTs. We recognized that perhaps in time, as federation IR matures, we can make some things into MUSTs, but for now this doc aims to be informative and inclusive; hence, no MUSTs that may limit participation in IR.
- Talked a lot about ambiguity associated with the various roles addressed in these procedures. Does everyone involved in an IR know all of the others who have some role in it? Does everyone involved know how to directly or indirectly message others in their management of the incident? Marina and Romain will get together to address this before next WG call.
- Returned once again to the wish for tooling that supports communication among those participating in an IR.

Along the way the WG decided to recommend that fed ops security contacts should be a requirement of eduGAIN participation. Tom will send Nicole that recommendation.